Criminal Justice Information Systems Administrative Information Use Policy

Criminal Justice Information Systems "Administrative Information" is recognized as any data related to the business of criminal justice. JUSTIS recognizes administrative information to be a resource that requires proper management in order to permit effective planning and decision-making and to conduct business in a timely and effective manner.

Administrative information does not include financial or personnel data. It includes, but is not limited to, data maintained at local, federal, and municipal criminal justice agencies that specifically address defendant and offender data.

Participating criminal justice agencies retain ownership of all "administrative information" created or modified by their employees and subsequently electronically provided to the JUSTIS System. As such, owner agencies are responsible for the accuracy, timeliness, and completeness of all data being or to be shared.

Classification of Data

For security purposes, criminal justice administrative information can be categorized into four levels of protection:

Confidential

- Confidential information is information that requires a high level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration, or destruction of the data. Improper use or disclosure of this information could adversely affect the ability of criminal justice agencies to accomplish their mission. Confidential information also includes records about individuals requiring protection under the Privacy Act of 1974 and data not permitted to be released under the Freedom of Information Act.

Sensitive

- Sensitive information is information that requires some level of protection, because its unauthorized disclosure, alteration, or destruction will cause perceivable damage to criminal justice agencies or the individual(s) of record. It is assumed that all administrative information output from criminal justice agency computer centers or central computing facilities is classified as sensitive unless otherwise indicated. Health-related information should be considered sensitive.

Non-Sensitive/Private

- Non-sensitive/private information is information that is intended for use within criminal justice agencies and the criminal justice community at-large. Its unauthorized disclosure could adversely impact criminal justice agencies, its employees, and or the individual(s) of record. This information should be made available on a need-to-know basis only and is not intended for public access.

Unrestricted/Public

- Unrestricted information is information that can generally be made available both within and beyond the criminal justice community. Public information is information that does not fit into any of the above categories. Its unauthorized disclosure may be against policy, but it is not expected to seriously or adversely impact criminal justice agencies, its employees, or the individual(s) of record.

Data Security Policy

Criminal justice administrative information is the most valuable resource of the JUSTIS system and requires responsible use by members of the criminal justice community. Employees are charged with safeguarding the integrity, accuracy, and confidentiality of this information as part of the condition of participation in the JUSTIS system. Employees are expected to act in a manner that will ensure the information which they are authorized to access is protected from unauthorized access, unauthorized use, invalid changes, or destruction. Access to the JUSTIS system is granted to a particular individual based on the need to use specific data as defined by job duties, and is subject to appropriate approval. This access cannot be shared, transferred, or delegated. Failure to protect this resource may result in disciplinary measures being taken against the employee, up to and including termination and or prosecution.

Definition of Security

Information is secure only when its integrity can be maintained, its availability ensured, its confidentiality preserved, and its access controlled. Security procedures protect information from unauthorized viewing, modification, dissemination, or destruction and provide recovery mechanisms from accidental loss. The security of criminal justice administrative information is the responsibility of all criminal justice practitioners who are authorized to access it.

Data Access

The following provisions detail the responsibilities of employees in maintaining the security of criminal justice administrative information. Employees are also subject to the laws, regulations, and policies contained in:

- NCIC Security Policy
- Title 28; Chapter 1 Part 20
- Section 4-131 through 4-137 of the annotated code of the District of Columbia
- Section 1004 of the DC Manual of Regulations
- Rules of Behavior included in the JUSTIS User Access Request/Registration Request package
- Agency guidelines specific to the information that is accessed

The following sections define responsibilities, establish authorization, and provide guidelines to assist people in the handling of criminal justice resource information.

JUSTIS System Users

The term “employees” is used in the most general sense to incorporate any and all persons who perform services and are granted access to criminal justice administrative information. The term does not in and of itself confer any special status or relationship with criminal justice agencies and is not intended to confer employee status. In addition to regular staff, the term employee includes full-time staff, temporary staff, contractual staff, consultants, and volunteers.

Employees are responsible for the security of criminal justice administrative data. While these guidelines provide examples of appropriate care, they are not intended to be exhaustive of all activities that ensure this security. Staff are expected to evaluate their actions with respect to the protection of administrative data and to act in a manner which is in the best interest of the criminal justice agency where they are employed.

The term "supervisor" is used in the most general sense to incorporate not only people whose job function is defined to include supervision of staff but also to apply to people who informally direct the work of others. Such titles as supervisor, manager, director, chairperson, department head, etc., are used to formally denote supervisors; however, many other positions are also supervisory (e.g., uniform personnel).

It is the responsibility of supervisors to maintain a high level of security in the work place. Supervisors have a responsibility to inform their staff of the proper manner of handling criminal justice administrative information, to evaluate the effectiveness of these procedures, and recommend changes to improve this security.

The term "chairperson/department head" is used to denote the director of an administrative unit. Their responsibility in this regard is to support procedures related to the security of data and data resources. Chairpersons/department heads should review office procedures annually and make updates in response to changes in technology and policies. Annual budgets should anticipate the need for funding of resources to protect criminal justice administrative information located in the department or agency.

All agencies participating in the sharing of information and whose intent is to utilize that data for criminal justice purposes shall agree to hold its employees to the same security standards and rules of behavior regardless of rank or agency hierarchy. JUSTIS does not make any attempt to dictate and/or designate responsibility to any agency or its employees in this regard.

Information Technology Security Officer(s)

Information Technology Security Officers constitute a body of knowledgeable users who function as trustees of their agency's criminal justice administrative information as it
relates to the JUSTIS System. For each agency maintaining an information application within JUSTIS, an Information Technology Security Officer (ITSO) should be selected and assigned the authority for making decisions related to access of that agency's application(s) via JUSTIS, and the data associated with that business function. Information Technology Security Officers are responsible for enforcing the established guidelines for the management and protection of the data. In addition, ITSO's are responsible for:

- conducting internal audits for the purpose of evaluating compliance with information security policies and procedures established by JUSTIS;
- evaluating the effectiveness of security procedures and other agency controls to limit access to JUSTIS information;
- and, reviewing audit trails to determine if activity is adequately documented, allowing for improprieties to be identified and corrected.

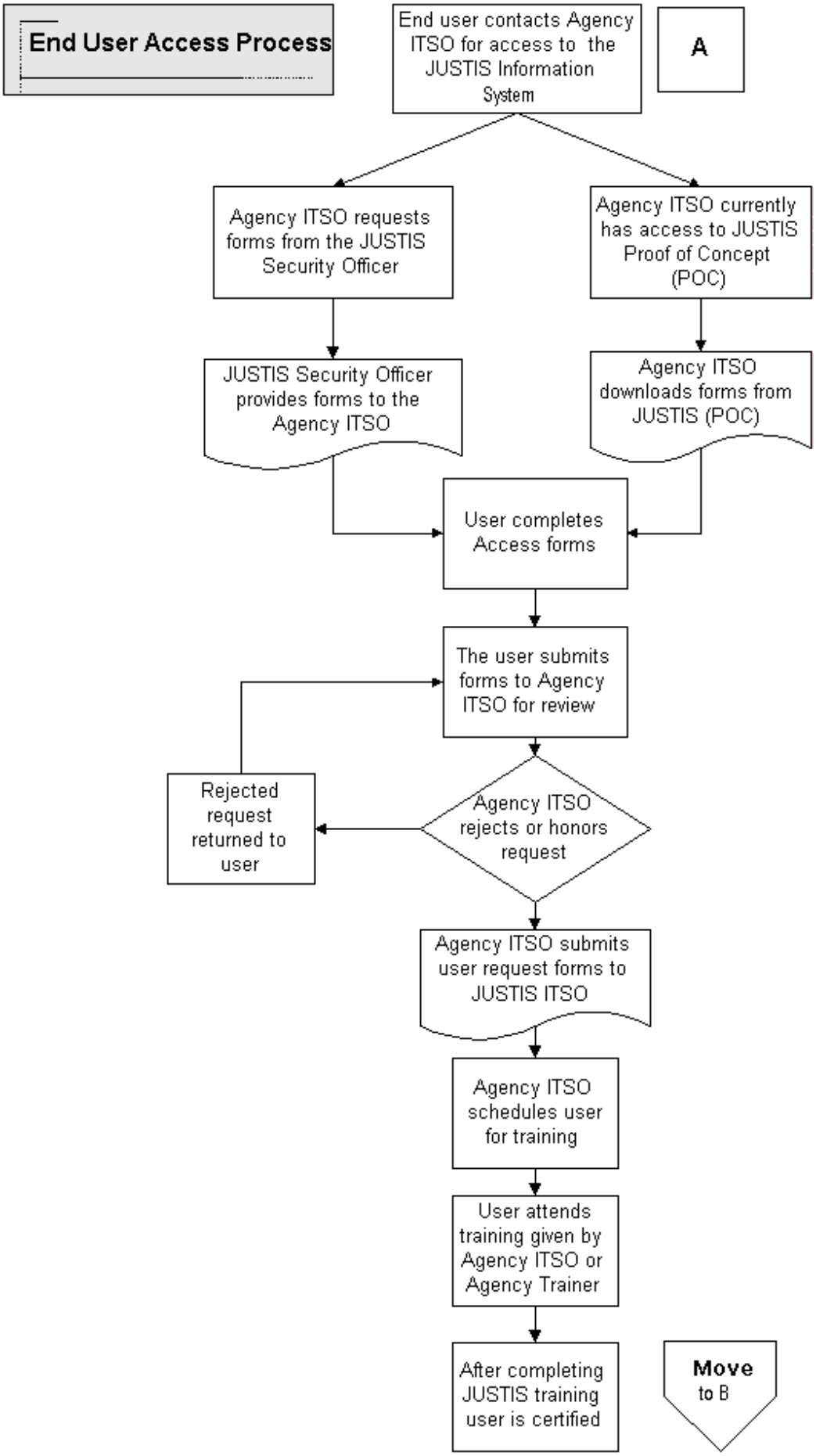
Information Technology Services Staff

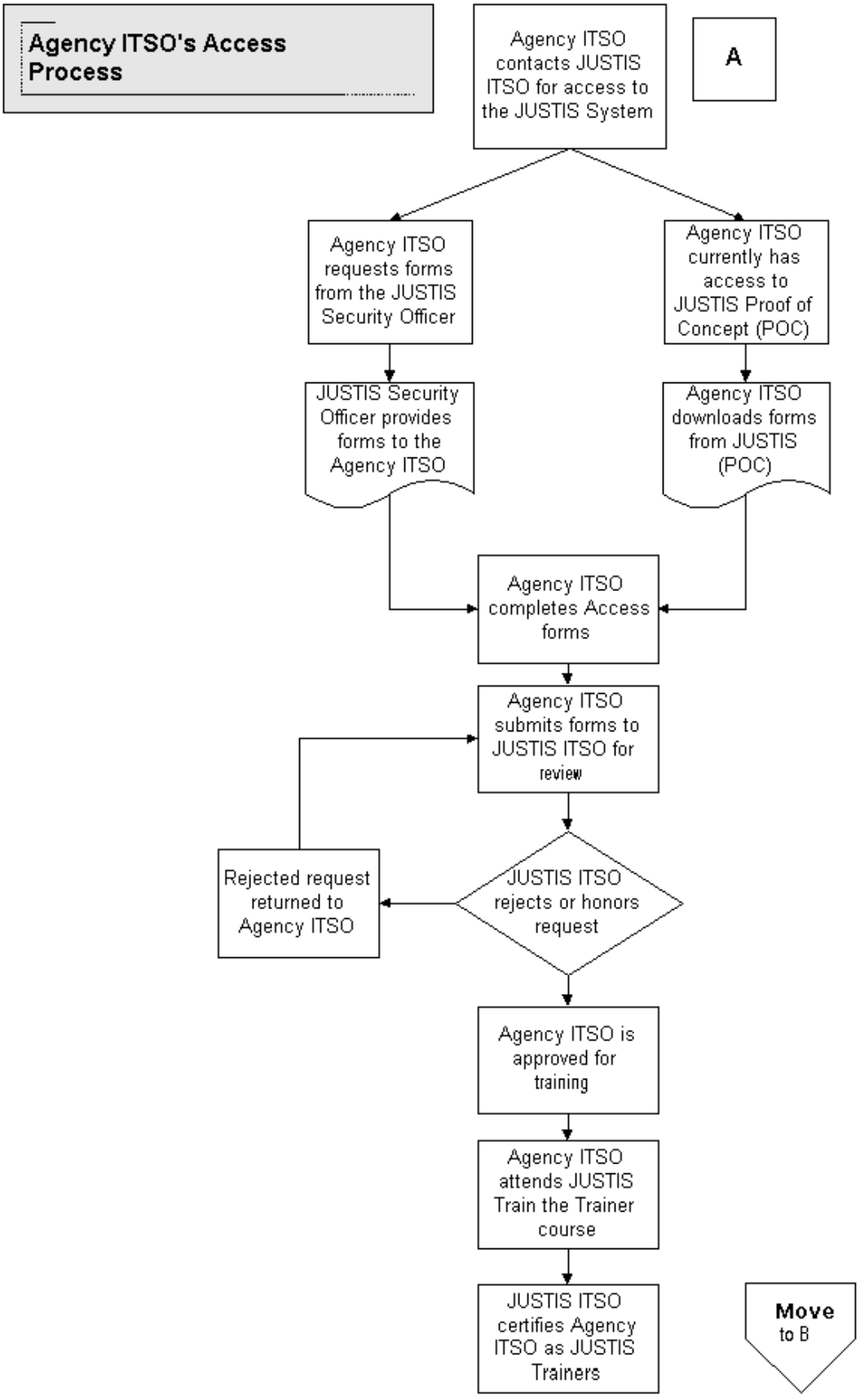
Information Technology Services (ITS) staff have the expertise and the responsibility to protect administrative criminal justice information residing on agency mainframes, networks, and local servers. ITS staff must use this expertise in a responsible manner to ensure the integrity of the data and the availability of the information provided electronically to the JUSTIS system.

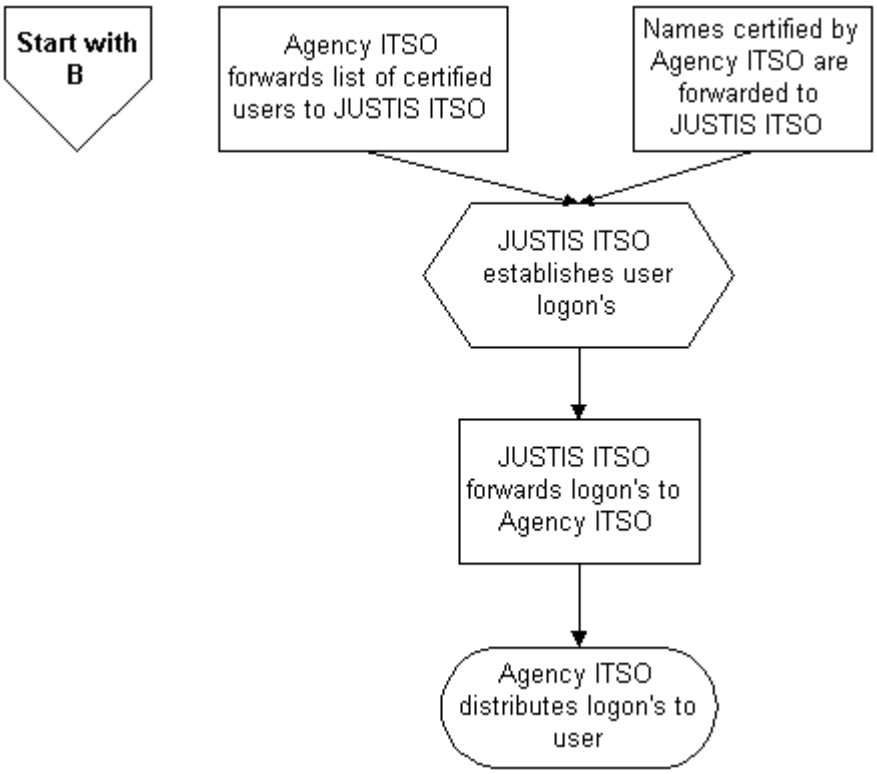
Procedures for Access to the JUSTIS System

Requests for access to electronic information must be made using the appropriate forms. Access to the JUSTIS System must be made using the User Access Registration/Request Form Package which is only available from the JUSTIS Information Technology Security Officer. Each form must include sufficient information to determine why an employee needs the requested access and the signatures of required authorized administrators.
Access procedures are as follows:

- User Access Registration/Request forms will be issued to agency Information Technology Security Officers (ITSO) or Information Technology Advisory Committee (ITAC) members for dissemination to prospective users.
- Upon completion of all forms, the "authorization for release of information" form will be maintained by the respective agency ITSO and utilized for authorization purposes.
- Authorized users who have received an FBI clearance will be scheduled for JUSTIS training.
- Initial JUSTIS training for agency trainers will be conducted by the JUSTIS ITSO. Subsequent training will be conducted by agency ITSO's and agency trainers who will provide training to personnel of their respective agencies.
- Access Registration/Request forms will be forwarded to the JUSTIS ITSO by the respective agency ITSO. Absolutely **no** applications will be accepted from individual users.
- The JUSTIS ITSO will provide the user with a password/logon via the appropriate agency ITSO.
- The JUSTIS ITSO will maintain an electronic database of all users and passwords/logons for audit purposes.


End User Access Process
End user contacts Agency ITSO for access to the JUSTIS Information System
A
Agency ITSO requests forms from the JUSTIS Security Officer
Agency ITSO currently has access to JUSTIS Proof of Concept (POC)
JUSTIS Security Officer provides forms to the Agency ITSO
Agency ITSO downloads forms from JUSTIS (POC)
User completes Access forms
The user submits forms to Agency ITSO for review
Agency ITSO rejects or honors request
Rejected request returned to user
Agency ITSO submits user request forms to JUSTIS ITSO
Agency ITSO schedules user for training
User attends training given by Agency ITSO or Agency Trainer
After completing JUSTIS training user is certified
Move to B


Agency ITSO's Access Process
Agency ITSO contacts JUSTIS ITSO for access to the JUSTIS System
A
Agency ITSO requests forms from the JUSTIS Security Officer
Agency ITSO currently has access to JUSTIS Proof of Concept (POC)
JUSTIS Security Officer provides forms to the Agency ITSO
Agency ITSO downloads forms from JUSTIS (POC)
Agency ITSO completes Access forms
Agency ITSO submits forms to JUSTIS ITSO for review
JUSTIS ITSO rejects or honors request
Rejected request returned to Agency ITSO
Agency ITSO is approved for training
Agency ITSO attends JUSTIS Train the Trainer course
JUSTIS ITSO certifies Agency ITSO as JUSTIS Trainers
Move to B


Start with B
Agency ITSO forwards list of certified users to JUSTIS ITSO
Names certified by Agency ITSO are forwarded to JUSTIS ITSO
JUSTIS ITSO establishes user logon's
JUSTIS ITSO forwards logon's to Agency ITSO
Agency ITSO distributes logon's to user